I

109TH CONGRESS
1ST SESSION

H. R. 3140

To expand the protections for sensitive personal information in Federal law to cover the information collection and sharing practices of unregulated information brokers, to enhance information security requirements for consumer reporting agencies and information brokers, and to require consumer reporting agencies, financial institutions, and other entities to notify consumers of data security breaches involving sensitive consumer information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 30, 2005

Ms. BEAN (for herself, Mr. DAVIS of Alabama, Mr. FRANK of Massachusetts, Mrs. MALONEY, Mr. GUTIERREZ, Mr. WATT, Mr. ACKERMAN, Mr. FORD, Mr. CROWLEY, Mr. CLAY, Mrs. MCCARTHY, Mr. LYNCH, Ms. WASSERMAN SCHULTZ, and Ms. MOORE of Wisconsin) introduced the following bill; which was referred to the Committee on Financial Services

---

A BILL

To expand the protections for sensitive personal information in Federal law to cover the information collection and sharing practices of unregulated information brokers, to enhance information security requirements for consumer reporting agencies and information brokers, and to require consumer reporting agencies, financial institutions, and other entities to notify consumers of data security breaches involving sensitive consumer information, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Consumer Data Security and Notification Act of 2005''.

SEC. 2. AMENDMENTS TO THE FAIR CREDIT REPORTING ACT.

(a) FCRA COVERAGE OF DATA BROKERS.—Section 603(d) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)) is amended by adding at the end the following new paragraph:

''(4) COMMUNICATION OF PERSONALLY IDENTIFIABLE INFORMATION BY CERTAIN PERSONS INCLUDED.—The term 'consumer report' shall also include any written, oral, electronic, or other communication of any information by any person which, for monetary fees, dues or other compensation, regularly engages in whole or in part in the practice of assembling or evaluating personally identifiable information for the purpose of furnishing reports to third parties that includes the name of any consumer and any of the following information relating to such consumer:

''(A) Any Social Security account number.

''(B) Any driver's license number.

''(C) Any other identification number issued by a State or the Federal Government.

''(D) Any bank, savings association, credit union, or investment account number.

''(E) Any credit card, or debit card account number.

''(F) Any password, access code, or security code relating to a bank, savings association, credit union, or investment account number or credit or debit card account number.''.

(b) VERIFICATION STANDARDS FOR USERS OF CONSUMER REPORTS.—Section 604(f) of the Fair Credit Reporting Act (15 U.S.C. 1681b(f)) is amended—

(1) by striking ''and'' at the end of paragraph (1);

(2) by redesignating paragraph (2) as paragraph (3); and

(3) by inserting after paragraph (1) the following new paragraph:

''(2) the identity of the person requesting the consumer report has been verified, pursuant to section 607(a), in accordance with procedures which the Commission shall prescribe in regulation; and''.

(c) DATA SECURITY STANDARDS AND NOTIFICATION OF SECURITY BREACHES.—

(1) IN GENERAL.—The Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) is amended by adding at the end the following new section:

"SEC. 630. PROTECTION OF NONPUBLIC CONSUMER INFORMATION.

''(a) IN GENERAL.—Notwithstanding any other provision of this title, each consumer reporting agency shall have an affirmative and continuing obligation to respect the privacy of consumers and to protect the security and confidentiality of consumers nonpublic personal information.

''(b) SAFEGUARDS REQUIRED.—In furtherance of subsection (a), the Commission shall establish appropriate standards, by regulation, for consumer reporting agencies relating to administrative, technical, and physical safeguards—

''(1) to insure the security and confidentiality of consumer records and information;

''(2) to protect against any anticipated threats or hazards to the security of such records; and

''(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

''(c) NOTIFICATION OF DATA SECURITY BREACHES.—

''(1) IN GENERAL.—The regulations prescribed under subsection (b) shall include requirements for the notification of consumers following the discovery of a breach of security of any data system maintained by the consumer reporting agency in which sensitive consumer information was, or is reasonably believed to have been, acquired by an unauthorized person.

''(2) CONTENT OF REGULATIONS.—The regulations prescribed under paragraph (1) shall include the following requirements or provisions:

''(A) A requirement that a consumer reporting agency provide written notice to a consumer whenever such agency becomes aware that sensitive personal information relating to the consumer has been, or is reasonably believed to have been, acquired by an unauthorized person, unless the consumer reporting agency, after appropriate investigation—

''(i) reasonably concludes that misuse of the information is unlikely to occur;

''(ii) notifies the appropriate law enforcement agency of the data security breach; and

''(iii) takes appropriate steps to remedy the security breach and safeguard the interests of affected consumers.

''(B) A requirement that the notices required under paragraph (1) be provided by a consumer reporting agency without unreasonable delay following—

''(i) the discovery by such agency of a breach of security in the data system; and

''(ii) reasonable actions which the consumer reporting agency shall take to investigate the nature and intent of the breach, prevent further unauthorized access or disclosure, and restore the reasonable integrity of the data system.

''(C) A provision that allows for reasonable delay of such notification to the consumer under paragraph (1) upon the written request of a law enforcement agency which has determined that the notification required under paragraph (1) would seriously impede a criminal investigation.

''(D) A provision that the written notice required under paragraph (1) may be made by an electronic transmission only if—

''(i) the consumer has provided prior consent to receive any such notice by electronic transmission; and

''(ii) the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act.

''(E) A requirement that the notification provided to consumers include—

''(i) the date on which the consumers nonpublic personal information was, or is reasonably believed to have been, acquired by an unauthorized person;

''(ii) the specific information that was, or is reasonably believed to have been, acquired by an unauthorized person, including Social Security account numbers, bank or investment account numbers, credit or debit card account numbers, or any password or code relating to such accounts;

''(iii) the actions taken by the consumer reporting agency to address or remedy the security breach and prevent unauthorized use of nonpublic personal information;

''(iv) the summary of rights of consumer victims of fraud or identity theft prepared by the Federal Trade Commission under section 609(d) and information on how to contact the Commission for more detailed information; and

''(v) the toll-free telephone number where consumers may obtain additional information about the security breach and an explanation of available options to protect their consumer file from unauthorized access.

''(3) TREATMENT OF ENCRYPTED INFORMATION.—For purposes of the regulations prescribed under paragraph (1), the Commission shall—

''(A) permit a consumer reporting agency, in connection with any determination pursuant to paragraph (2)(A)(i), to reasonably conclude that misuse of information is unlikely to occur where the sensitive consumer information ac-

quired, or believed to have been acquired, by an unauthorized person consists of information that has been encrypted in a manner consistent with standards set forth under subparagraph (B);

''(B) identify appropriate standards for encryption of personal and financial information for purposes of subparagraph (A), taking into consideration the Advanced Encryption Standard adopted by the National Institute of Standards and Technology for use by the Federal Government; and

''(C) establish appropriate criteria for determining whether information that has been encrypted has been accessed by an unauthorized person, and whether misuse of such information is likely to occur and notification is required pursuant to this section.''.

(2) CLERICAL AMENDMENT.—The table of contents for the Fair Credit Reporting Act is amended by inserting after the item relating to section 129 the following new item:

''630. Protection of nonpublic consumer information.''.

(d) USE OF CONSUMER REPORTS FOR PRIVATE INVESTIGATIONS.—

(1) IN GENERAL.—Section 604(a)(3) of the Fair Credit Reporting Act (15 U.S.C.1681b(a)(3)) is amended—

(A) by striking ''or'' at the end of subparagraph (E);

(B) by redesignating subparagraph (F) as subparagraph (G); and

(C) by inserting after subparagraph (E) the following new paragraph:.

''(F) is a duly licensed private investigator who intends to use the consumer report only in connection with a lawful investigation within the scope of the investigator's license and for no other purpose; or''.

(2) TECHNICAL AND CONFORMING AMENDMENT.—Section 603(k)(1)(B)(iv)(I) of the Fair Credit Reporting Act (15 U.S.C. 1681a(k)(1)(B)(iv)(I)) is amended by striking ''604(a)(3)(F)(ii)'' and inserting ''604(a)(3)(G)(ii)''.

(e) REGULATIONS.—The Federal Trade Commission shall prescribe such regulations as the Commission determines to be necessary to implement the amendments made by this section and such regulations shall be published in final form before the end of the 6-month period beginning on the date of the enactment of this Act.

SEC. 3. AMENDMENTS TO TITLE V OF THE GRAMM-LEACH-BLILEY ACT.

(a) NOTIFICATION OF SECURITY BREACHES.—Section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801) is amended by adding at the end the following new subsection:

''(c) NOTIFICATION OF DATA SECURITY BREACHES.—

''(1) IN GENERAL.—In establishing standards pursuant to subsection (b), each agency or authority described in section 505(a) shall require, in regulation, that a financial institution notify customers following the discovery of a breach of security of any data system maintained by the financial institution in which nonpublic personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

''(2) CONTENT OF REGULATIONS.—The regulations prescribed under paragraph (1) shall include the following requirements or provisions:

''(A) A requirement that a financial institution provide written notice to a customer whenever the institution becomes aware that sensitive personal information relating to the customer has been, or is reasonably believed to have been, acquired by an unauthorized person,

unless the financial institution, after appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur, and—

''(i) promptly notifies its primary Federal financial regulatory agency of the data security breach;

''(ii) notifies the appropriate law enforcement agency of the data security breach; and

''(iii) takes appropriate steps to remedy the security breach and safeguard the interests of affected customers, including monitoring the affected customers accounts for unusual or suspicious activity.

''(B) A requirement that the notice required under paragraph (1) be provided by a financial institution without unreasonable delay following—

''(i) the discovery by the financial institution of a breach of security in the data system;

''(ii) reasonable investigation of the nature and scope of the security breach, including identification of the customer in-

formation systems and specific customer information or accounts that may have been accessed;

''(iii) notification of the primary Federal financial regulatory agency for the financial institution;

''(iv) notification of appropriate law enforcement agencies; and

''(v) reasonable measures to prevent further unauthorized access or disclosure and to restore the reasonable integrity of the data system.

''(C) A provision establishing minimum standards for investigations of the nature and scope of security breaches, including any limitation on the duration of such investigations that the agency or authority may consider appropriate to prevent substantial harm or inconvenience to any customer;

''(D) A provision that allows for reasonable delay of such notification upon the written request of a law enforcement agency which has determined that the notification required under paragraph (1) would seriously impede a criminal investigation;

''(E) A provision that the written notice required under paragraph (1) may be made by an electronic transmission only if—

''(i) the customer has provided prior consent to receive any such notice by electronic transmission; and

''(ii) the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act.

''(F) A requirement that the notification provided to consumers include—

''(i) the date on which the customers nonpublic personal information was, or is reasonably believed to have been, acquired by an unauthorized person;

''(ii) the specific information that was, or is reasonably believed to have been, acquired by an unauthorized person, including Social Security account numbers, bank or investment account numbers, credit or debit card account numbers, or any password or code relating to such accounts;

"(iii) the actions taken by the financial institution to address or remedy the security breach and prevent unauthorized use of nonpublic customer information;

"(iv) the summary of rights of consumer victims of fraud or identity theft prepared by the Federal Trade Commission under section 609(d) of the Fair Credit Reporting Act and information on how to contact the Commission for more detailed information; and

"(v) the toll-free telephone number where customers may obtain additional information about the security breach and explanations of available options to protect their consumer file from unauthorized access.

"(G) A requirement concerning any other action or disclosure that the agency or authority determines necessary or appropriate to carry out the intent of this subsection.

"(3) CERTAIN PERSONS TREATED AS FINANCIAL INSTITUTIONS FOR THIS SUBSECTION.—

"(A) IN GENERAL.—For purposes of this subsection (and sections 504, 505, and 507 to

the extent applicable with respect to this subsection), the term 'financial institution' includes any person or organization that, in the regular course of business, collects and maintains written or electronic files containing individually identifiable information on customer transactions, including any bank, savings association, or credit union account number, credit card or debt card number, and any other payment account number, or any password, access code, or security code pertaining to any such account or any credit card or debit card.

''(B) NOTIFICATION.—A person or organization described in subparagraph (A) that is required to provide written notice pursuant to regulations prescribed under paragraph (1), shall, promptly notify the appropriate law enforcement agency of the data security breach, and provide notification, as appropriate—

''(i) to the customer whose payment account information has been, or is reasonably believed to have been, acquired by an unauthorized person, and such notification includes all applicable disclosures required by paragraph (2)(F);

"(ii) to the financial institution which is the holder of the customer's bank, savings association, or credit union account, credit card or debit card account, or other payment account which has been, or is reasonably believed to have been, acquired by an unauthorized person, which shall be in such form and include such information as required by regulation; or

"(iii) to the financial intermediary or network used to effect the credit transaction, electronic fund transfer, or other form of payment on behalf of the customer whose payment account information has been, or is reasonably believed to have been, acquired by an unauthorized person, which shall include the information required by subparagraph (C) and such other information as required by regulation.

"(C) RESPONSE OF FINANCIAL INTERMEDIARY OR NETWORK UPON RECEIVING NOTICE.— A financial intermediary or network that receives notice of a data security breach pursuant to subparagraph (B)(iii) shall prompt-

ly communicate to the financial institution which is the holder of the bank, savings association, or credit union account, credit card or debit card account, or other payment account with respect to which such breach occurred, all necessary information pertaining to the data security breach, which shall include the date on which the breach is reasonably believed to have occurred and the name and location of the person or organization responsible for maintaining the data system where the security breach occurred.

''(D) RESPONSE OF FINANCIAL INSTITUTION THAT HOLDS CUSTOMER'S ACCOUNT UPON RECEIVING NOTICE.—A financial institution that receives notice of a data security breach pursuant to subparagraphs (B)(ii) or (C) may communicate to any customer whose bank, savings association, or credit union account, credit card or debit card account, or other payment account is identified as having been, or is reasonably believed to have been, acquired by an unauthorized person, any information it receives relating to the security breach, including the date on which the breach is reasonably believed

to have occurred and the name and location of the person or organization responsible for maintaining the data system where the security breach occurred.

''(E) FINANCIAL INTERMEDIARY OR NETWORK DEFINED.—For purposes of this paragraph, the term 'financial intermediary or network' means a credit card association, electronic fund transfer network, or other system, clearinghouse, or network utilized by any creditor, credit card issuer, financial institution, or money transmitting business, to effect a credit transaction, electronic fund transfer, or other money transmitting, check clearing, or payment service.

''(4) TREATMENT OF ENCRYPTED INFORMATION.—The regulations prescribed under paragraph (1) shall—

''(A) permit a financial institution, in connection with any determination pursuant to paragraph (2)(A), to reasonably conclude that misuse of information is unlikely to occur where the sensitive consumer information acquired, or believed to have been acquired, by an unauthorized person consists of information that has

been encrypted in a manner consistent with standards set forth under subparagraph (B);

''(B) identify appropriate standards for encryption of personal and financial information for purposes of subparagraph (A), taking into consideration the Advanced Encryption Standard adopted by the National Institute of Standards and Technology for use by the Federal Government; and

''(C) establish appropriate criteria for determining whether information that has been encrypted has been accessed by an unauthorized person, and whether misuse of such information is likely to occur and notification is required pursuant to this section.''.

(b) REGULATIONS.—The agencies and authorities described in section 505(a) of the Gramm-Leach-Bliley Act shall, in the manner prescribed in section 504 of such Act, prescribe such regulations as the agencies and authorities determine to be necessary to implement the amendments made by this section and such regulations shall be published in final form before the end of the 6-month period beginning on the date of the enactment of this Act.

○